					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P02S					Dokumendi pealkiri: **Juhtimisrollide ja vastutuste poliitika**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kohaldatavate standardite ja õigusaktidega kooskõla

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 5	
ISO/IEC 27002:2022	Kontrollimeetmed: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
EL GDPR	Artiklid 5(2), 32	

1. Eesmärk

1.1 Käesolev poliitika määratleb, kuidas organisatsioonis infoturbe juhtimisega seotud vastutused määratakse, delegeeritakse ja hallatakse, et tagada täielik vastavus standardile ISO/IEC 27001:2022 ning muudele regulatiivsetele kohustustele.

1.2 See tagab vastutuste selguse kõigil tasanditel ning toetab tegevuse tulemuslikkust, määratledes üheselt, kes vastutab iga turvalisusega seotud funktsiooni eest.

1.3 Käesolev poliitika toetab auditivalmidust ja suurendab klientide usaldust, tõendades formaalse infoturbe juhtimise olemasolu ka organisatsioonides, kus tehniline personal on piiratud või IT-teenused on sisse ostetud.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile isikutele, kes käitlevad organisatsiooni süsteeme või andmeid, sealhulgas:

2.1.1 Ärivaldkonna omanikud ja tegevjuhid

2.1.2 Töötajad ja töövõtjad

2.1.3 Välised IT-teenuse osutajad või konsultandid

2.2 See hõlmab kõiki süsteeme, keskkondi ja teenuseid, mida kasutatakse äri- või klienditeabe töötlemiseks, edastamiseks või säilitamiseks, sealhulgas:

2.2.1 Kontori IT-taristu ja kaugtööseadmed

2.2.2 Pilvepõhised platvormid ja e-posti teenused

2.2.3 Füüsilised dokumendid ja ühiskettad

2.3 Kohaldamisala hõlmab nii sisemisi kui ka sisse ostetud tegevusi, mis on seotud infoturbe juhtimisega.

3. Eesmärgid

3.1 Kehtestada selge vastutus kõigi turvalisusega seotud ülesannete eest, sealhulgas poliitikate halduse, pääsukontrolli, intsidentide käsitlemise ja seire eest.

3.2 Tagada tööülesannete tõhus lahusus, et vähendada huvide konflikti või pettuse riski.

3.3 Tagada, et turbeülesanded ja rollid on selgelt dokumenteeritud ning vaadatakse regulaarselt üle.

3.4 Toetada teadlikku otsustamist, eskaleerimist ning IT- ja turberiskide järelevalvet.

3.5 Toetada ISO/IEC 27001:2022 sertifitseerimist ning suurendada klientide, partnerite ja audiitorite usaldust.

4. Rollid ja vastutused

4.1 Tegevjuht / ettevõtte omanik

4.1.1 Vastutab täielikult käesoleva poliitika rakendamise ja järelevalve eest.

4.1.2 Kinnitab kõik turberollid, vastutused ja delegeerimisotsused.

4.1.3 Jälgib vastavust ning teeb lõplikud otsused poliitika erandite ja eskalatsioonide kohta.

4.2 Määratud turbekoordinaator (kui see on määratud)

4.2.1 Võib olla töötaja või usaldusväärne konsultant.

4.2.2 Mikroettevõtte keskkonnas võib seda rolli täita tegevjuht või väline teenuseosutaja.

4.2.3 Toetab igapäevaselt pääsukontrolli rakendamist, intsidendiohjet või põhiliste tehniliste turbeülesannete täitmist.

4.2.4 Teatab kõigist turbeprobleemidest või riskidest viivitamata tegevjuhile.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane läbivaatamine

9.1.1 Tegevjuht peab käesoleva poliitika iga 12 kuu järel üle vaatama, et tagada selle jätkuv vastavus õiguslikele kohustustele, tegevusvajadustele ja ISO/IEC 27001 sertifitseerimise nõuetele.

9.2 Vahepealsed läbivaatamised

9.2.1 Läbivaatamine tuleb teha ka siis, kui:

9.2.1.1 Toimuvad olulised organisatsioonilised muudatused

9.2.1.2 Kaasatakse uus teenuseosutaja

9.2.1.3 Toimub tõsine turvaintsident

9.2.1.4 Uuendatakse regulatiivseid nõudeid, nagu GDPR, NIS2 või DORA

9.3 Versioonihaldus ja dokumenteerimine

9.3.1 Kõik läbivaatamised peavad sisaldama järgmist:

9.3.1.1 Läbivaatamise kuupäev

9.3.1.2 Muudatuste kokkuvõte

9.3.1.3 Tegevjuhi allkiri või dokumenteeritud kinnitus

9.3.1.4 Arhiveeritud varasemad versioonid auditi tarbeks

9.4 Muudatuste teatavakstegemine

9.4.1 Kõigist poliitika uuendustest tuleb töötajaid ja teenuseosutajaid viivitamata teavitada e-posti, siseportaali või ametlike teadete kaudu.

10. Seotud poliitikad ja seosed

10.1 Täieliku tulemuslikkuse tagamiseks tuleb käesolevat poliitikat rakendada koos järgmiste SME-poliitikatega:

10.1.1 P4S – Pääsukontrolli poliitika: määratleb, kuidas juurdepääsu antakse, hallatakse ja lõpetatakse ning on otseselt seotud määratud rollide ja järelevalvega.

10.1.2 P8S – Infoturbe teadlikkuse ja koolituse poliitika: tugevdab rollipõhiseid vastutusi ja ootusi.

10.1.3 P17S – Andmekaitse ja privaatsuse poliitika: kirjeldab GDPR-ist tulenevaid õiguslikke kohustusi, mis määratakse käesolevas juhtimispoliitikas määratletud rollidele.

10.1.4 P30S – Intsidendiohje poliitika: nõuab määratletud vastutusi intsidendidest teatamiseks, nende eskaleerimiseks ja lahendamiseks.

10.2 Koos võimaldavad need poliitikad järjepideva rakendamise, sisemise vastutuse selguse ja välise vastavuse.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 5.3 – Organisatsiooni rollid, vastutused ja volitused: nõuab, et rollid oleksid selgelt määratletud ja tippjuhtkonna toetatud.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeetmed 5.2–5.4: nõuavad infoturbe rollide selget dokumenteerimist, tööülesannete lahusust ja juhtimistasandi järelevalvet.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: kehtestab üldise infoturbeprogrammi koos määratletud vastutustega.

11.3.2 PL-1 kuni PL-4: nõuavad planeerimise kontrollimeetmeid, sealhulgas poliitikate koostamist ja dokumenteeritud rollimääranguid.

11.3.3 CA-1: nõuab määratletud hindamis- ja volitusrolle.

11.3.4 AC-1: seob rollipõhise pääsukontrolli määratud juhtimisvastutustega.

11.4 EL GDPR

11.4.1 Artikkel 5(2) – Vastutuse põhimõte: nõuab, et organisatsioon suudaks tõendada vastavust rollide ja vastutuste kaudu.

11.4.2 Artikkel 32 – Töötlemise turvalisus: rõhutab ülesannete selget määratlemist isikuandmete kaitsmiseks.

11.5 EL NIS

11.5.1 Artikkel 21(2)(a): nõuab juhtimisstruktuure, mis hõlmavad formaliseeritud rolle küberriskide ja intsidentide haldamiseks.

11.6 EL DORA

11.6.1 Artiklid 9 ja 10: nõuavad, et finantssektori üksused määraksid selgelt IKT- ja turvalisusega seotud vastutused ning teostaksid nende üle järelevalvet.

11.7 COBIT 2019

11.7.1 EDM03 – Riski optimeerimise tagamine: nõuab turberiski juhtimiseks selgelt määratletud rolle ja eskalatsiooniteid.

11.7.2 APO13 – Turvalisuse juhtimine: määrab strateegilised ja operatiivsed turbeülesanded isikutele ja rollidele.

11.7.3 DSS05 – Turbeteenuste juhtimine: nõuab väliste ja sisemiste turbeteenuste vastutustes struktuuri ja jälgitavust.